FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1496258-0

Total Deleted Page(s) = 3
Page 8 ~ b6; b7C; b7E;
Page 9 ~ b6; b7C; b7E;
Page 12 ~ b5; b6; b7C;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

[redacted] b3 b7E

FD-71 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Complaint Form

Title: (U) Access Industries, Inc. e-mail intrusion **Date:** 02/10/2015

Approved By: SSA [redacted] b3 b6 b7C b7E

Drafted By: [redacted]

Case ID #: [redacted] (U) MENDEZ SUPREME TRADES INC. ; EMAIL INTRUSION; VICTIM: ACCESS INDUSTRIES, INC.;

Complaint Synopsis: (U) Email intrusion for the purpose of conducting unauthorized wire transfers.

Full Investigation Initiated: 02/10/2015

Received On: 02/09/2015

Receipt Method: In Person

Incident Type: Criminal Activity

Complaint Details:

On or about December 13, 2014 unknown person(s) logged into the a corporate e-mail account [redacted] owned by ACCESS INDUSTRIES, INC (ACCESS INC)without permission or authority. b6 b7C

Once logged into the account, the unknown person(s) made unauthorized email-handling rule changes to the account. The rule changes caused approximately 1,490 emails to be forwarded to an identified external email address. The rule also caused emails received from MERRILL LYNCH and BANK OF AMERICA to be deleted after being forwarded.

On or about December 22, 2014 an email was sent to MERRILL LYNCH from the ACCESS INC email address. The email requested MERRILL LYNCH send a $49,800.60 wire to TD BANK account holder, MENDEZ SUPREME TRADES

Title: (U) Access Industries, Inc. e-mail intrusion
Re: [redacted] 02/10/2015

INC., account number [redacted] b6 b7C

MERRILL LYNCH requested verbal confirmation from ACCESS INC for the wire request. ACCESS INC identified the wire request email as unauthorized and alerted MERRILL LYNCH.

MERRILL LYNCH cancelled the wire request, resulting in no financial losses.

Entities:

Access Industries, Inc. (Complainant, Organization, U.S. Person? Unknown)

Location

Address: 730 fifth Avenue
City: New York
State: NY
Zip Code: 10019
Country: United States

Financial Account

Type: Security
Institution: Merrill Lynch
Association: Uses

Communication Account

Type: Email
Account: [redacted] b6 b7C
Association: Utilizes

TD Bank (Reference, Organization, U.S. Person? Unknown)

Financial Account

Mendez Supreme Trades Inc. (Reference, Organization, U.S. Person? Unknown)

Location

Address: 5946 Madison Street
Apartment 1
City: Ridgewood

State: NY
Zip Code: 11385
Country: United States
Association: Residence

Communication Account
Type: Telephone
Account: 347-232-2882

Financial Account
Type: Bank
Account: [redacted]
Institution: TD Bank
Association: Uses

b6
b7C

BANK OF AMERICA (Reference, Organization, U.S. Person? Unknown)
Financial Account

MERRILL LYNCH (Reference, Organization, U.S. Person? Unknown)
Organization Information
Name: MERRILL LYNCH
Type: Corporation

♦♦

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 02/18/2015

Meeting conducted with representatives of ACCESS INDUSTRIES, INC (ACCESS INC) for the purpose of reviewing information regarding a e-mail intrusion and attempted unauthorized wire transfer. Information as follows:

Meeting was conducted at ACCESS INC, New York, corporate office located at 730 Fifth Avenue, New York, New York, 10019.

Representatives/Task Force Officer's (TFO) present during meeting are as follows:

- [redacted] ACCESS INC, [redacted]
- [redacted] ACCESS INC,
- [redacted] CASALE ASSOCIATES, LLC, [redacted]
- [redacted] ESQ. CASALE ASSOCIATES, LLC, Attorney Investigator. b6 b7C
- [redacted] TFO JTCTF
- [redacted] TFO JTCTF
- [redacted] TFO JTCTF

[redacted] explained the following events leading to an attempted unauthorized wire request:

On December 22, 2014 ACCESS INC [redacted] received a telephone call from a representative of MERRILL LYNCH. The representative requested a verbal confirmation for a $49,800.60 transfer request received via email [redacted] knowing he did not send the request asked the representative to send a copy of the email back to his [redacted] email. [redacted] waited for the email to arrive in his email inbox. After waiting for a time [redacted] contacted MERRILL LYNCH and inquired about the email. [redacted] was informed that the email was sent. [redacted] conducted a search of his email account and found the email in the accounts deleted items folder. b6 b7C

also notified ACCESS INC , of the incident. conducted a internal review of email account. found that new email processing rules were created on email account. The rules, which were created on or about December 13, 2014, caused emails from ML.COM (MERRILL LYNCH) and BANKOFAMERICA.COM (BANK OF AMERICA) to be automatically deleted. Additional review by found that all emails sent to were being forwarded to an email account identified as Both email processing rules were made without knowledge or permission.

On or about December 24, 2014 disabled the unauthorized email processing rules. also changed his email password to comply with a strong password policy.

reviewed the email sent to MERRILL LYNCH requesting the wire transfer. determined that the email was sent directly from mailbox hosted at MICROSOFT OFFICE 365 cloud services and originated form IP . An IP search confirmed that the IP is owned by TIME WARNER CABLE.

conducted a review of the email attachment sent to MERRILL LYNCH on 12/22/2014. determined that the attachment was most likely used by for a prior legitimate email wire transfer request. The attachment was downloaded from email account on an unknown date and time. Reviewing metadata also determined that the legitimate transfer was modified using MICROSOFT WORD 2013, on 12/22/2014 at 2:28:30 PM by author "TECHIE". The document was then converted into a PFF using Neevia Document Converter Pro v6.7, before being emailed to MERRILL LYNCH.

explained that ACCESS INC. is currently using a Hybrid email system as the company migrates to a fully cloud based email service provided by MICROSOFT 365. ACCESS INC currently manages 100 corporate emails, 30 of which are cloud based. The remaining 70 accounts are traditional server based emails. email is cloud based. Login information is administrated and documented by MICROSOFT.

provided a copies of the following:

- EMAIL HEADER (MRRILL LYNCH EMAIL SENT 12/22/2014)
- ATTACHMENT TO MERRILL LYNCH EMAIL
- NOTES REGARDING INCIDENT
- Corporate MICROSOFT account#

1. On December 22, 2014 [redacted] has received a call from his Merrill Lynch financial advisor with the request to confirm wire transfer from one of his accounts in amount of ~$44,5K that was allegedly was sent earlier by email.
2. [redacted] has requested a copy of this email to be sent back to him for review.
3. After waiting some time and noticing that expected email is not arriving to his Inbox, [redacted] has found this email in his Deleted Items folder. He has contacted me with the request to look into this situation. b6 b7C
4. After login remotely into [redacted] home PC and further investigation, we (me and [redacted] have determined that number of malicious automatic email processing rules were created in his mailbox. These rules were forwarding all messages from ml.com to bankofamerica.com to email account at Russian free mobile email service provides ro.ru (Rumbler) and sequentially deleting these previously forwarded emails from [redacted] Inbox
5. We have disabled these email auto processing rules in [redacted] mailbox and he placed a call to his Merrill Lynch advisor with the request to forward message in question to my email address as an attachment, to preserve metadata.
6. After further metadata investigation of said message, we have determined that it was sent directly from [redacted] mailbox hosted at Microsoft Office 365 cloud services and was originated from IP [redacted] that resolved to [redacted] b6 b7C b7E
7. Based on finding s above [redacted] password was immediately changed, insuring that it is compliant with strong password policy.
8. Investigation of forged Wire Transfer Request metadata has reviled that this document was created by author "Techie" with Microsoft Word 2013 on 12/22/2014 at 2:28:30 PM and converted into PFF with Neevia Document Converter Pro v 6.7. As per [redacted] perpetrators most likely have used and modified legitimate Wire Transfer Request that was earlier prepared by him and sent to Merrill Lynch for execution. b6 b7C

OCEAN TERRACE HOLDINGS
VENDOR PAYMENT AUTHORIZATION & WIRE INSTRUCTIONS

VENDOR: MENDEZ SUPREME TRADES INC

INVOICE NO.: 1419-09-14 DATE: 12.15.14

AMOUNT DUE: $49,800.60

VENDOR PAYMENT BY RESPONSIBLE PARTY: [redacted]

SANDOR SCHER: $4,980.06 [redacted] $44,820.54

APPROVED BY: [redacted] DATE: 12/15/14

b6
b7C

VENDOR WIRE TRANSFER INFORMATION:

MENDEZ SUPREME TRADES INC
c/o TD Bank Bronx,NY
ABA no [redacted]
Account Number [redacted]
Ref: Payment of Inv no 1419-09-14 for services rendered

b6
b7C

COMPLETED:_____ BY:_____

Merrill Lynch

12-22-14

Please pay by wire the attached invoice for

1. **$44,820.54 (forty-one thousand eight hundred and twenty dollars and 54 Cents)**

From my credit line.

Reference: From [redacted] for Ocean Terrace Holdings

b6
b7C

[redacted]

Thanks, [redacted]

[redacted]

b3
b7E

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: EMAIL **Date:** 03/03/2015

Title: (U) Identified victim in [redacted]

b3
b6
b7C
b7E

Approved By: SSA [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) MENDEZ SUPREME TRADES INC. ;
EMAIL INTRUSION;
VICTIM: ACCESS INDUSTRIES, INC.;

Synopsis: (U) This E-mail serves to document an identified victim in the captioned case. A victim notification letter will be mailed to the victim.

♦♦

UNCLASSIFIED

Sent: Monday, March 02, 2015 3:00 PM
Subject: RE: Recently opened cases --- UNCLASSIFIED

Classification: UNCLASSIFIED
==========

[redacted]	2/10/2015	NY-CY06	[redacted]	Pending

b3 b6 b7C b7E

Hello [redacted]
In case [redacted] the victim has been identified as **Access Industries Inc.**, 730 Fifth Avenue, New York, NY, 10019. Access Industries Inc. Legal contact information [redacted]

From: [redacted] (NY) (FBI)
Sent: Thursday, February 26, 2015 12:49 PM
To: [redacted]

b6 b7C

Cc: [redacted] (NY) (FBI)
Subject: Recently opened cases --- UNCLASSIFIED

Classification: UNCLASSIFIED
==========

Good Afternoon, everyone.

Please find your case below.

As the Victim Specialist assigned to your squad, I must follow up every month with new possible-victim cases to ensure you're in compliance with federal law. In other words, I want to keep you off a HQ list for non-compliance.

Remember – possible federal crime victims must be notified of their rights as soon as reasonably possible and before an indictment.

Please advise if:

- *You have any possible federal crime victims in your case*
- *If I may send a victim notification letter to the victim(s)*
- *If sending a victim notification letter to a known victim would interfere with your investigation or the victim's security*
- *If the case is classified:*
  - *Secret*
  - *FBI isn't the lead agency*
  - *The crime was determined to not be a federal offense*
  - *Restricted*
  - *Victim is a government entity*
  - *Other (please explain)*

Please E-mail me back by Tuesday, March 3.

Also, I welcome your call if you wish to discuss any victim issues.

Thank you very much and I hope your week is a good one.

Sincerely,

[redacted] b6 b7C

Victim Specialist	File #	Date opened	Squad	Special Agent	Status
[redacted]	50-NY-6059188	1/30/2015	NY-C2	[redacted]	Pending
	318B-NY-6094015	2/2/2015	NY-C35		Pending
	194B-NY-6096500	2/4/2015	NY-C4		Pending
	194C-NY-6110543	2/10/2015	NY-C4		Pending
	318B-NY-6096142	2/3/2015	NY-C43		Pending
	15-NY-6111620	2/13/2015	[redacted]		Pending
	[redacted]	1/16/2015	NY-CY06		Pending
		2/10/2015	NY-CY06		Pending
		2/11/2015	NY-CY06		Pending

b3 b6 b7C b7E

[redacted] MA
Victim Specialist
FBI New York/JFKRA
[redacted] (desk)
(mobile)

==========
Classification: UNCLASSIFIED

==========
Classification: UNCLASSIFIED

[redacted] MA
Victim Specialist
FBI New York/JFKRA
[redacted] (desk)

b6 b7C b7E

[redacted] (mobile)

b6
b7C
b7E